Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

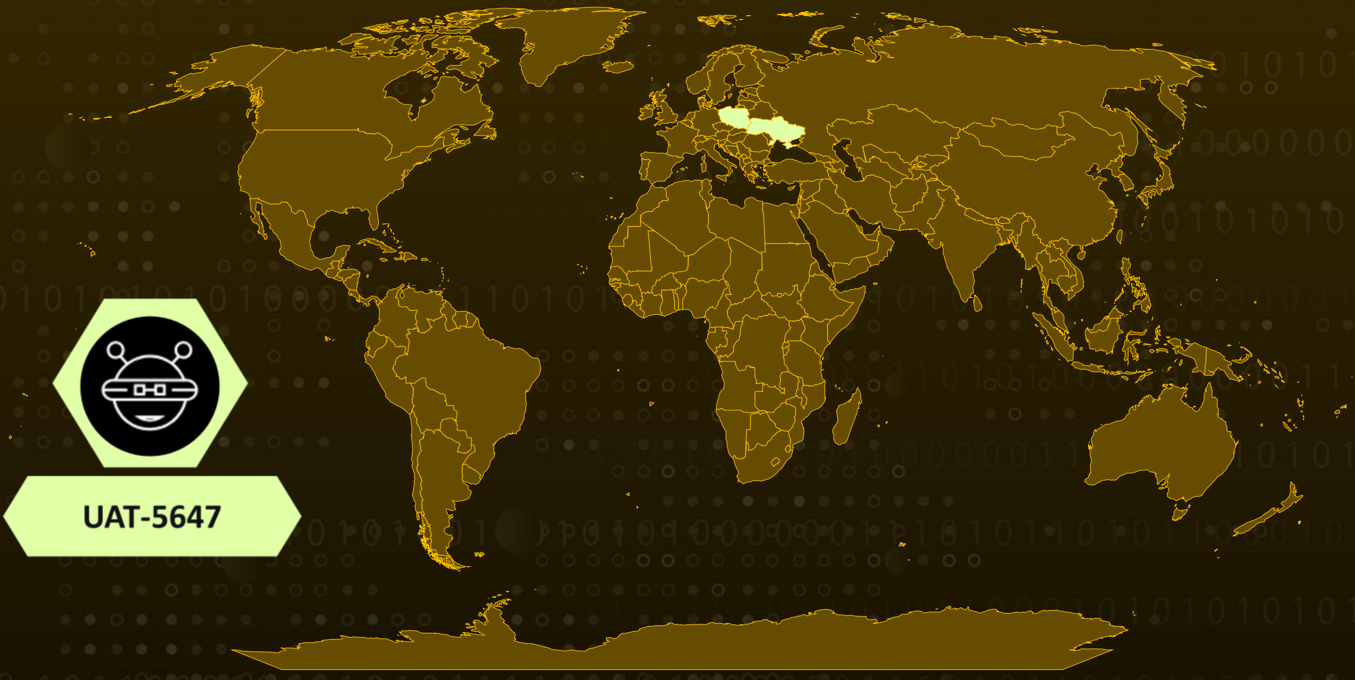
UAT-5647 Unleashes New Malware Arsenal in Targeted Espionage Campaigns

Date of Publication	Admiralty Code	TA Number
October 18, 2024	A1	TA2024400

Summary

Attack Discovered: Late 2023
Targeted Countries: Ukraine and Poland
Targeted Industries: Government
Actor: UAT-5647 (aka RomCom, Tropical Scorpius, Void Rabisu, DEV-0978, Storm-0978)
Malware: SingleCamper (aka RomCom RAT, RomCom, SnipBot, RomCom 5.0), RustClaw, MeltingClaw, DustyHammock, ShadyHammock
Attack: The Russian cybercriminal group UAT-5647 (also known as RomCom) has launched a new wave of cyberattacks targeting Ukrainian government agencies and unidentified Polish entities since late 2023. These attacks involve a new variant of the RomCom RAT, now known as SingleCamper (also referred to as SnipBot or RomCom 5.0). UAT-5647 has also expanded their toolkit to include four distinct malware families, two downloaders identified as RustClaw and MeltingClaw, two backdoors named DustyHammock and ShadyHammock. This evolution of their tools reflects a more sophisticated approach, allowing them to carry out persistent and targeted attacks with greater stealth and complexity.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

The Russian cybercriminal group UAT-5647, also known as RomCom, has intensified its cyberattacks, primarily targeting Ukrainian government agencies and expanding into Polish entities. These operations serve dual purposes, establishing long term espionage footholds and potentially deploying ransomware for financial gain. UAT-5647 has evolved its malware toolkit, incorporating multiple programming languages such as GoLang, C++, RUST, and LUA, allowing for more sophisticated and versatile attacks.

#2

The infection chain typically begins with spear-phishing emails containing malicious attachments disguised as important documents. These attachments house one of two downloaders, RustClaw or MeltingClaw, which act as the first stage of the attack. Once executed, these downloaders install backdoors like DustyHammock and ShadyHammock. These backdoors enable the attackers to establish persistent access to the compromised systems, allowing for continued infiltration, data exfiltration, and the execution of additional malicious payloads.

#3

RustClaw, a RUST based downloader, checks system characteristics, such as keyboard layout, to ensure it targets specific geographies like Ukraine or Poland. It uses hash matching techniques to evade sandbox detection, and after verification, it downloads the next stage malware, DustyHammock. MeltingClaw operates similarly, delivering ShadyHammock and other payloads, such as SingleCamper (aka **SnipBot**), a variant of the RomCom RAT. These backdoors then communicate with a command-and-control (C2) server, executing reconnaissance commands and enabling further attacks.

#4

Once inside a network, UAT-5647 conducts extensive post compromise activities. The attackers show a particular interest in network reconnaissance, scanning for exposed systems and network shares. They use tools like PuTTY's Plink to establish remote tunnels, enabling them to infiltrate deeper into the network while remaining undetected. The group's goal appears to be long term access, allowing them to steal sensitive data and prepare for potential ransomware deployment.

#5

To counter these advanced tactics, organizations should take several proactive steps which will help detect and block malicious activities early in the infection chain. As UAT-5647 continues to evolve its techniques and expand its malware capabilities, organizations in targeted regions must remain vigilant and proactive in defending against these increasingly sophisticated cyberattacks.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Monitoring network traffic: It is essential to Monitoring network traffic for unusual activity is a crucial step in defending against advanced cyberattacks. Organizations should pay close attention to connections involving suspicious external IP addresses or domains, especially those associated with InterPlanetary File System (IPFS) or other decentralized file-sharing systems, which threat actors like UAT-5647 may use to exfiltrate data or distribute additional payloads.

Network Segmentation: To enhance protection against evolving threats, organizations should implement multi-layered security controls. One critical strategy is network segmentation, which isolates sensitive systems and data, reducing the risk of lateral movement in case of a breach

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment	T1572 Protocol Tunneling
T1016 System Network Configuration Discovery	T1135 Network Share Discovery	T1033 System Owner/User Discovery	T1614 System Location Discovery

T1614.001 System Language Discovery	**T1082** System Information Discovery	**T1482** Domain Trust Discovery	**T1083** File and Directory Discovery
T1069 Permission Groups Discovery	**T1069.001** Local Groups	**T1012** Query Registry	**T1560** Archive Collected Data
T1003 OS Credential Dumping	**T1104** Multi-Stage Channels	**T1070** Indicator Removal	**T1059** Command and Scripting Interpreter
T1059.001 PowerShell			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	12bf973b503296da400fd6f9e3a4c688f14d56ce82ffcfa9edddd7e4b6b93ba9, 260a6644ab63f392d090853ccd7c4d927aba3845ced473e13741152cdf274bbd, 9062d0f5f788bec4b487faf5f9b4bb450557e178ba114324ef7056a22b3fbe8b, 43a15c4ee10787997682b79a54ac49a90d26a126f5eeeb8569022850a2b96057, aa09e9dca4994404a5f654be2a051c46f8799b0e987bcefef2b52412ac402105, 585ed48d4c0289ce66db669393889482ec29236dc3d04827604cf778c79fda36, 62f59766e62c7bd519621ba74f4d0ad122cca82179d022596b38bd76c7a430c4, 9fd5dee828c69e190e46763b818b1a14f147d1469dc577a99b759403a9dadf04, b1fe8fbbb0b6de0f1dcd4146d674a71c511488a9eb4538689294bd782df040df, 7602e2c1ae27e1b36ee4aed357e505f14496f63db29fb4fcdd0d8a9db067a5c4, f3fe04a7e8da68dc05acb7164b402ffc6675a478972cf624de84b3e2e4945b93, 10e1d453d4f9ca05ff6af3dcd7766a17ca1470ee89ba90feee5d52f8d2b18a4c, a265ae8fed205efb5bcc2fb59e60f743f45b7ad402cb827bc98dee397069830c, 8104fdf9ff6be096b7e5011e362400ee8dd89d829c608be21eb1de959404b4b9,

TYPE	VALUE
SHA256	b55f70467f13fbad6dde354d8653d1d6180788569496a50b06f2ece1f57a5e91, bd25618f382fc032016e8c9bc61f0bc24993a06baf925d987dcec4881108ea2a, 78eaaf3d831df27a5bc4377536e73606cd84a89ea2da725f5d381536d5d920d8, 88a4b39fb0466ef9af2dcd49139eaff18309b32231a762b57ff9f778cc3d2dd7, 01ebc558aa7028723bebd8301fd110d01cbd66d9a8b04685afd4f04f76e7b80c, 7c9775b0f44419207b02e531c357fe02f5856c17dbd88b3f32ec748047014df8, 54ce280ec0f086d89ee338029f12cef8e1297ee740af76dda245a08cb91bab4d, bf5f2bdc3d2acbfb218192710c8d27133bf51c1da1a778244617d3ba9c20e6f7, fdbc6648c6f922ffcd2b351791099e893e183680fc86f48bf18815d8ae98a4f7, ac9e3bf1cc87bc86318b258498572793d9fb082417e3f2ff17050cf6ec1d0bb5, 0a02901d364dc9d70b8fcdc8a2ec120b14f3c393186f99e2e4c5317db1edc889, 951b89f25f7d8be0619b1dfdcc63939b0792b63fa34ebfa9010f0055d009a2d3, 2e338a447b4ceaa00b99d742194d174243ca82830a03149028f9713d71fe9aab, 45adf6f32f9b3c398ee27f02427a55bb3df74687e378edcb7e23caf6a6f7bf2a, B9677c50b20a1ed951962edcb593cce5f1ed9c742bc7bff827a6fc420202b045, ce8b46370fd72d7684ad6ade16f868ac19f03b85e35317025511d6eeee288c64, 9f635fa106dbe7181b4162266379703b3fdf53408e5b8faa6aeee08f1965d3a2, 1fa96e7f3c26743295a6af7917837c98c1d6ac0da30a804fed820daace6f90b0, dee849e0170184d3773077a9e7ce63d2b767bb19e85441d9c55ee44d6f129df9, 2474a6c6b3df3f1ac4eadcb8b2c70db289c066ec4b284ac632354e9dbe488e4d
IPv4	213[.]139[.]205[.]23, 23[.]94[.]207[.]116, 91[.]92[.]242[.]87, 192[.]227[.]190[.]127, 91[.]92[.]254[.]218,

TYPE	VALUE
IPv4	91[.]92[.]248[.]75, 94[.]156[.]68[.]216, 193[.]42[.]36[.]131, 23[.]137[.]253[.]43, 193[.]42[.]36[.]132
URLs	hxxp[:]//apisolving[.]com:443/DKgitTDJfiP, hxxp[:]//wirelesszone[.]top:433/OfjdDebdjas, hxxp[:]//adcreative[.]pictures:443/kjLY1Ul8IMO, hxxp[:]//creativeadb[.]com:443/n9JTcP62OvC
Domains	dnsresolver[.]online, apisolving[.]com, rdcservice[.]org, webtimeapi[.]com, wirelesszone[.]top, devhubs[.]dev, pos-st[.]top, adcreative[.]pictures, creativeadb[.]com, copdaemi[.]top, adbefnts[.]dev, store-images[.]org

References

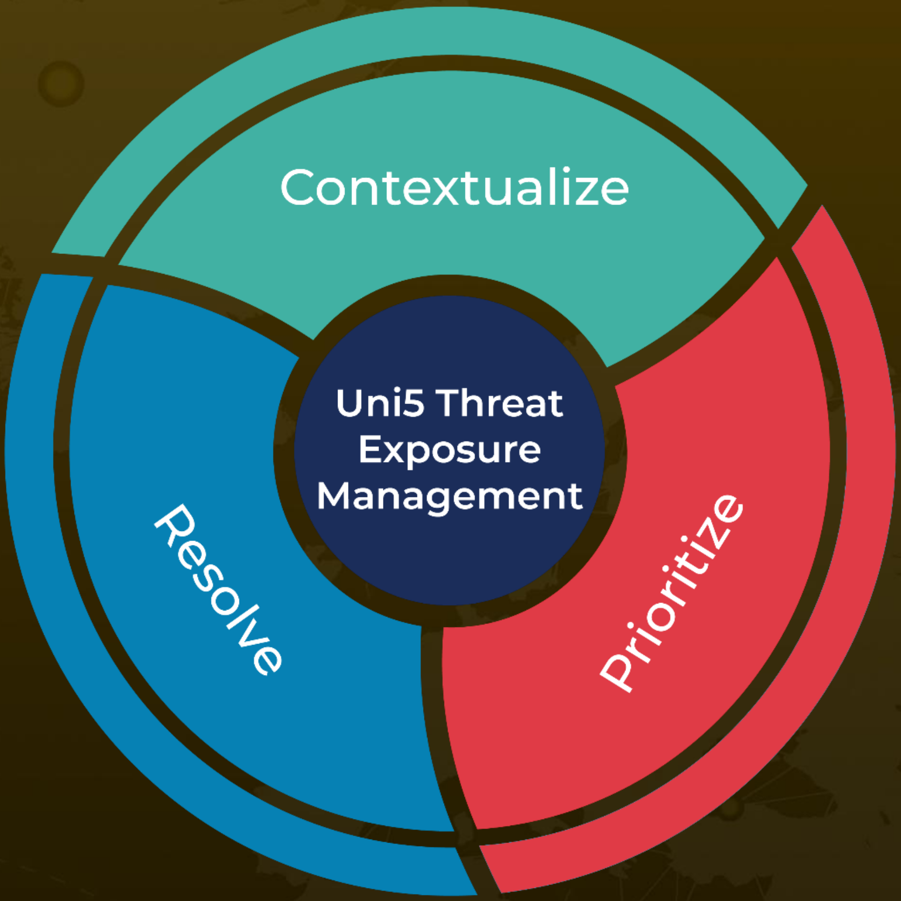
https://blog.talosintelligence.com/uat-5647-romcom/

https://hivepro.com/threat-advisory/snipbot-unpacking-the-latest-romcom-malware-variant/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 18, 2024 • 7:20 AM

More at www.hivepro.com